IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Massimiliano Antonio Poletto et al.	Art Unit	: 2113
Serial No.	: 10/701,154	Examiner	: Elmira Mehrmanesh
Filed	: November 3, 2003	Conf. No.	: 5561
Title	: CONNECTION BASED ANOMALY DETECTION		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF ON BEHALF OF MASSIMILIANO ANTONIO POLETTO ET AL.

The Brief fee of **$270** is being paid concurrently on the electronic filing system by way of deposit account authorization. Please apply any other charges or credits to Deposit Account No. 06-1050.

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: January 22, 2009

(1) Real Party in Interest

The real party in interest in the above application is Mazu Networks, Inc.

(2) Related Appeals and Interferences

Appellant is not aware of any appeals or interferences related to the above-identified patent application.

(3) Status of Claims

This is an appeal from the decision of the Primary Examiner in a final office action dated **August 6, 2008**, finally rejecting claims 1-3, 5, 7-16, 18-22, and 28-32.

Claims 4 and 6 were canceled. Claims 23-27 and 33-36 were indicated as allowed.

Appellant filed a Notice of Appeal on **December 18, 2008**. Claims 1-3, 5, 7-16, 18-22, and 28-32 are the subject of this Appeal.

(4) Status of Amendments

Appellant filed a Reply to the Final Office Action. In an advisory action dated Jan 14, 2009, the examiner indicated that the amendments would not be entered. The proposed amendments were directed to matters of form not affecting basis of Appellant's argument. All previously filed amendments have been entered.

(5) Summary of Claimed Subject Matter

Claim 1

Appellant's claim 1 is directed to a system. See FIGS. 1 and 2. Also, "*Referring to FIG. 1, an anomaly detection system 10 to detect anomalies and process anomalies into events is shown.*"[1]

Inventive features of Appellant's claim 1 include a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network. "*Referring to FIG. 2, collectors 12 are shown disposed to*

[1] Specification page 6, lines 16-17.

sample or collect information from network devices 15, e.g., switches as shown.."[2] *... Over a defined interval (typically 30 seconds), the data collectors 12 monitor all connections between all pairs of hosts and destinations using any of the defined protocols. At the end of each interval, these statistics are summarized and reported to the aggregator 14.*[3]

Inventive features of Appellant's claim 1 also include an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node. *"Referring to FIG. 3, the aggregator 14 is a device (a general depiction of a general purpose computing device is shown) that includes a processor 30 and memory 32 and storage 34. Other implementations such as Application Specific Integrated Circuits are possible. The aggregator 14 includes a process 36 to collect data from collectors 12 and a process 38 to produce a connection table 40."*[4]

Inventive features of Appellant's claim 1 also include a process executed on the aggregator device to detect anomalies in connection patterns and a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies. *"In addition, the aggregator includes anomaly analysis and event process 39 to detect anomalies and process anomalies into events that are reported to the operator console or cause the system 10 to take action in the network 18. Anomalies in the connection table can be identified as events including denial of service attacks, unauthorized access attempts, scanning attacks, worm propagation, network failures, addition of new hosts, and so forth."*[5]

Claim 14

Appellant's claim 14 is directed to a method.

Inventive features of Appellant's claim 10 include sending connection information to an aggregator to identify host connection pairs collected from a plurality of collector devices.

---

[2] Specification page 7, lines 13-15.
[3] Id. page 8, lines 5-12.
[4] Id. page, 9, lines 21-27.
[5] Id. page 9, line 27 to page 10, line 3.

"*Periodically, the collector devices 12 send to the aggregator 14 a record of ... connections between every host pair observed by the collector 12, broken down by port and protocol.*"[6]

Inventive features of Appellant's claim 10 also include producing in the aggregator a connection table that maps each node on the network to a record that stores information about traffic to the node and traffic from the node, with the connection table including a plurality of entries that are indexed by source address. This feature finds support as the analogous feature of claim 1.

Claim 28

Claim 28 is directed to a storage medium storing a computer program product, the computer program product. "*.. the aggregator 14 is a device (a general depiction of a general purpose computing device is shown) that includes a processor 30 and memory 32 and storage 34.*"[7]

Inventive features of Appellant's claim 28 include instructions for causing a computer to collect connection information to identify host connection pairs from packets that are sent between nodes on a network *Over a defined interval (typically 30 seconds), the data collectors 12 monitor all connections between all pairs of hosts and destinations using any of the defined protocols. At the end of each interval, these statistics are summarized and reported to the aggregator 14.*[8] and produce a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node. *Referring to FIG. 3, the aggregator 14 is a device (a general depiction of a general purpose computing device is shown) that includes a processor 30 and memory 32 and storage 34. Other implementations such as Application Specific Integrated Circuits are possible. The aggregator 14 includes a process 36 to collect data from collectors 12 and a process 38 to produce a connection table 40.*"[9]

---

[6] Specification page 6, line 31 to page 7, line 5.
[7] Id. page 9, lines 21 to 24.
[8] Id. page 8, lines 5-12.
[9] Id. page, 9, lines 21-27.

Inventive features of Appellant's claim 28 also include instructions for causing a computer to detect anomalies in connection patterns. "*In addition, the aggregator includes anomaly analysis and event process 39 to detect* "[10]

Inventive features of Appellant's claim 28 also include instructions for causing a computer to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack. "... *and process anomalies into events that are reported to the operator console or cause the system 10 to take action in the network 18. Anomalies in the connection table can be identified as events including denial of service attacks, unauthorized access attempts, scanning attacks, worm propagation, network failures, addition of new hosts, and so forth.*"[11]

(6) The Ground of Rejection to be Reviewed on Appeal

Claims 1-3, 5, 7-16, 18-22, and 28-32 stand rejected under 35 U.S.C. 102 (e) as being anticipated by Ontiveros et al. (U.S. Pub 20020107953).

(7) Argument

Anticipation

"It is well settled that anticipation under 35 U.S.C. §102 requires the presence in a single reference of all of the elements of a claimed invention." *Ex parte Chopra*, 229 U.S.P.Q. 230, 231 (BPA&I 1985) and cases cited.

"Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

"This court has repeatedly stated that the defense of lack of novelty (i.e., 'anticipation') can only be established by a single prior art reference which discloses each and every element of the claimed invention." *Structural Rubber Prod. Co. v. Park Rubber Co.*, 223 U.S.P.Q. 1264, 1270 (Fed. Cir. 1984), citing five prior Federal Circuit decisions since 1983 including *Connell.*

---

[10] Specification page 9, lines 27-29.
[11] Id. page 9, line 29 to page 10, line 3.

In a later analogous case the Court of Appeals for the Federal Circuit again applied this rule in reversing a denial of a motion for judgment n.o.v. after a jury finding that claims were anticipated. *Jamesbury Corp. v. Litton Industrial Prod., Inc.*, 225 U.S.P.Q. 253 (Fed. Cir. 1985).

After quoting from *Connell*, "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim," 225 U.S.P.Q. at 256, the court observed that the patentee accomplished a constant tight contact in a ball valve by a lip on the seal or ring which interferes with the placement of the ball. The lip protruded into the area where the ball will be placed and was thus deflected after the ball was assembled into the valve. Because of this constant pressure, the patented valve was described as providing a particularly good seal when regulating a low pressure stream. The court quoted with approval from a 1967 Court of Claims decision adopting the opinion of then Commissioner and later Judge Donald E. Lane:

> [T]he term "engaging the ball" recited in claims 7 and 8 means that the lip contacts the ball with sufficient force to provide a fluid tight seal **** The Saunders flange or lip only sealingly engages the ball 1 on the upstream side when the fluid pressure forces the lip against the ball and never sealingly engages the ball on the downstream side because there is no fluid pressure there to force the lip against the ball. The Saunders sealing ring provides a compression type of seal which depends upon the ball pressing into the material of the ring. *** The seal of Saunders depends primarily on the contact between the ball and the body of the sealing ring, and the flange or lip sealingly contacts the ball on the upstream side when the fluid pressure increases. 225 U.S.P.Q. at 258.

Relying on *Jamesbury*, the ITC said, "Anticipation requires looking at a reference, and comparing the disclosure of the reference with the claims of the patent in suit. A claimed device is anticipated if a single prior art reference discloses all the elements of the claimed invention as arranged in the claim." *In re Certain Floppy Disk Drives and Components Thereof*, 227 U.S.P.Q. 982. 985 (U.S. ITC 1985).

Claims 1-3, 5, 7-16, 18-22, and 28-32 are not anticipated by Ontiveros.

Claims 1, 5, 7 and 28

For the purposes of this appeal only, Claims 1, 5, 7 and 28 stand or fall together. Appellant's claim 1 is representative of this group of claims.

Claim 1 requires the features of: "... a plurality of collector devices ... to collect connection information to identify host connection pairs from packets that are sent between nodes on a network; and an aggregator device ... which produces a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node, with the aggregator device ... to detect anomalies in connection patterns; and ...to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies."

The examiner cites to paragraphs [0003, 0008, 0024, 0026, 0037 and 0040] in Ontiveros as teaching various features of claim 1.

Ontiveros does not describe use of connection information in detecting anomalies

Appellant's claim 1 is directed to using connection information in a connection table in detection of anomalies that can be indicators of, e.g., denial of service attacks and scanning attacks. Ontiveros neither describes nor suggests at least the claimed connection table and the features of claim 1 that include the connection table.

The examiner relies principally on [0037] from Ontiveros to disclose the claimed connection table. Specifically, the examiner explains in response to Appellant's prior argument that: "**the Examiner respectfully disagrees and would like to point out to paragraph [0037] wherein Ontiveros discloses "...the preferred packet daemon creates memory references to each packet source Media Access Control (MAC) address in a hash table, wherein keys (which are the part or group of the data by which it is sorted, indexed and cataloged), are mapped to array positions**"

Appellant contends that memory references taught by Ontiveros are neither the connection table nor equivalent to the claimed connection table. Claim 1 therefore cannot be

anticipated by Ontiveros because the reference fails to disclose all of the elements of the claim arranged as in the claim.[12]

Indeed, these memory references do not specifically describe connection information, as the connection information is used in the features of the claims. Ontiveros [0037] is set forth below:

> **[0037] Referring now to FIG. 2, and the operation of the preferred packet daemon of the IDS, the preferred packet daemon creates memory references to each packet source Media Access Control (MAC) address in a hash table, wherein keys (which are the part or group of the data by which it is sorted, indexed and cataloged), are mapped to array positions. As a result of sorting in memory (i.e., processing copies of the data packets), each dedicated packet daemon can sort packet counts on each port at near real-time speed.**

Nothing in paragraph [0037] corresponds to the claimed connection table. To further support this contention, Ontiveros' Fig. 2 is reproduced below:

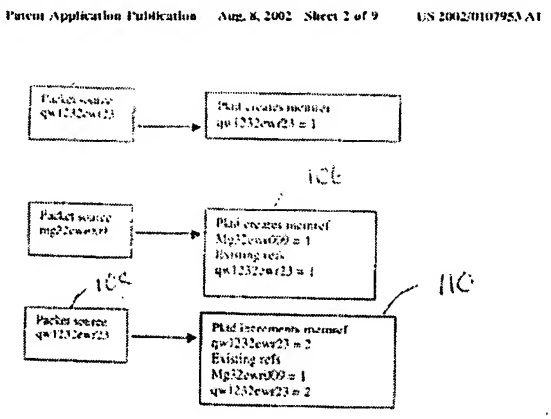

FIG. 2

As explained by Ontiveros, the memory references are storage areas for packet counts[13] in memory with a particular, e.g., source address. Ontiveros describes these memory references as:

---

[12] See *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

> **For example, as shown at 100 in FIG. 2, the packet daemon identifies the packet source address qw1232ewr23 and at 102 creates a memory reference (memref) for that source address. At 104 the packet daemon identifies the source address of the next data packet traversing the port being monitored by the packet daemon, in FIG. 2, the source address being mg32ewr009. At 106 another memref is created for this source address. Therefore, at 104 each of the memrefs are equal to 1, representing that one data packet from each of the sources identified has traversed the data port of interest.[14]**

Nothing in Fig. 2 paragraph [0037] or elsewhere shows that Ontiveros described the claimed connection table and specifically "host connection pairs from packets that are sent between nodes on a network; and an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node." That is, the structures of Fig. 2 of Ontiveros are not a record that stores information about packet traffic to the node and packet traffic from the node.

This is contrasted with Appellant's FIG. 4 a pictorial view of a connection table, which is reproduced below:

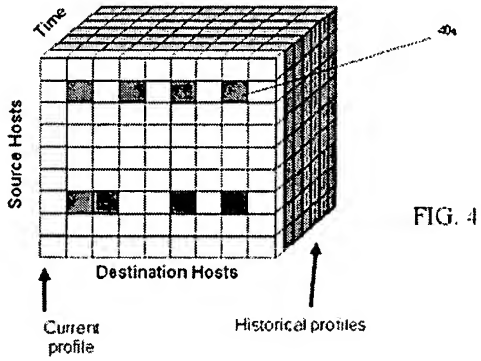

FIG. 4

and FIG. 5 (below) which depicts a representation of a record in the connection table of FIG. 4. As can be seen by the diagrammatical view of FIG. 4, the indices of the table are source and destination hosts over time periods.

In contrast, Ontiveros teaches at [0038] "**A "hit-count" table is preferably created in memory to count the number of times a particular pair of source and destination IP addresses is detected.**" Appellant contends that

---

[13] Ontiveros [0040] With respect more specifically to the "hit-count" table, each time a data packet is received, a preferred algorithm as described herein creates a new reference index (if one does not already exist) or increments the existing reference (i.e., counting packets).

[14] Id.

the teachings relied on by the examiner, namely [0037] are directed to this so called hit-count table which as Ontiveros describes keeps a count of the number of times a source address is detected.

However, nowhere does Ontiveros describe any structure similar to the record below, an example of a record in the connection table:

Time Slice	Fri	Thu	Wed	...	Sun	Sat	Fri
Services provided by A (Web Server) to B (Desktop)							
WWW (TCP:80)							
Bytes / sec	2k	3k	1k	...	2k	4k	3k
Packets / sec	5	6	2		5	9	5
Conn's. / hr	.3	.5	.3		.2	.3	.3
SSH (TCP:22)							
Bytes / sec	1k	3k	4k	...	1k	2k	3k
Packets / sec	2	6	9		2	5	6
Conn's. / hr	.3	.5	.3		.3	.3	.5
				...			
Services provided by B (Desktop) to A (Web Server)							
SSH (TCP:22)							
Bytes / sec	21k	0	0	...	0	0	0
Packets / sec	10	0	0		0	0	0
Conn's. / hr	1	0	0		0	0	0

FIG. 5

Therefore, Ontiveros cannot be construed to either describe or suggest "a connection table that maps each node on the network to a record that stores information about packet traffic to and from the node."

Ontiveros does not aggregate detected anomalies into network events

Appellant also contends that Ontiveros fails to describe a process to detect anomalies in connection patterns and a process to aggregate detected anomalies into network events.

The examiner contends that (paragraphs [0003], [0008], [0024] and [0026]) of Ontiveros disclose these features.

Paragraph [0003] discusses hackers and different types of attacks. Paragraphs [0008], [0024] and [0026] deal with teachings of Ontiveros as set forth below:

[0008] The invention is preferably provided as an intrusion detection system (IDS) using a packet daemon that captures, sorts, and catalogs network traffic on a packet-by-packet basis. The packets are preferably captured for inspection by an interface, for example, by using available libpcap libraries. These libraries are

> **further preferably used in connection with a parsing engine, which may be provided as a module that interfaces with the libpcap library (e.g., Practical Extraction and Reporting Language (Perl)). The combination results in a dynamically configurable firewall that can parse and trace network protocol hacking patterns using the capturing and parsing engines.**
>
> **[0024] Although the monitoring system 50 is preferably implemented using packet daemons 52 and is shown as implemented in a router 58, it may be provided in connection with other components of a network to thereby monitor data traffic. The monitoring system 50 of the present invention is preferably provided as a software and hardware adaptive firewall 54 addition to, for example, a switch router 58, which detects and denies data traffic with patterns that are in contrast to normal traffic patterns (i.e., exceed user defined configurable parameters), thereby preventing hacking attacks on networks. Depending upon the security requirements of the network, the present invention may be configured to detect different levels of attacks. The preferred packet daemon of the IDS 52 of the present invention uses the information it collects to issue firewall rules that make up the adaptive firewall functionality.**

In contrast to the claimed features, Ontiveros [0008] deals with an intrusion detection system (IDS) that uses a packet daemon that captures, sorts, and catalogs network traffic on a packet-by-packet basis. The packets are captured for inspection, parsing and tracing. In [0024] Ontiveros discusses specific implementations of packet daemons 52, e.g., as a software and hardware adaptive firewall 54; specifically that the daemon "**detects and denies data traffic with patterns that are in contrast to normal traffic patterns (i.e., exceed user defined configurable parameters), thereby preventing hacking attacks on networks.**" However, none of these teachings suggest the feature of claim 1 of "a process executed on the aggregator device to detect anomalies in connection patterns." Ontiveros deals with detection of traffic patterns, e.g., "**hit-count" table, each time a data packet is received, a preferred algorithm as described herein creates a new reference index (if one does not already exist) or increments the existing reference (i.e., counting packets)**, but not the feature of "connection patterns."

The examiner argues that Ontiveros teaches "a process executed on the aggregator device to aggregate detected anomalies into the network events (paragraph [0026]." Ontiveros discloses:

> **[0026] In the most preferred embodiment, six threads handle the various functions of the monitoring system 50. Specifically, the following threads are preferably provided: (1) Main Thread: initializes IDS data structures, activates the other threads, and waits for the other threads to complete their processes; (2) ADS connections thread: sends buffers to ADS, if ADS is present; (3) Packet Capture Thread: processes each packet, updates hit counts, queues lockout start commands to the per-second thread, extracts various fields, buffers the fields for transmission to an Anomaly Detection System (ADS), and notifies ADS connection thread to send buffers; (4) Per-second thread: runs each second, starts and stops lockout periods, and clears "hit" count table as configured; (5) Increment count thread: to determine a lock-out condition; and (6) Signal Catching Thread: re-reads configuration file, handles IDS 52 process cleanup and termination**

In [0026] Ontiveros discusses thread handling processing of the monitoring system 50. Claim 1, however, includes "a process to aggregate detected anomalies into the network events ... ." While Ontiveros discusses thwarting attacks, Ontiveros does not have any process that detects anomalies in connection patterns and determines whether the anomalies should be aggregated into events that can be associated with these types of attacks (thus minimizing false positives).

Claims 2 and 29

For the purposes of this appeal only, Claims 2 and 29 stand or fall together. Appellant's claim 2 is representative of this group of claims.

Claim 2 distinguishes over Ontiveros at least because Ontiveros neither describes nor suggests: "... wherein the aggregator determines at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusions.

Ontiveros detects intrusions from the counts not from connection patterns derived from the connection table.

Claims 3 and 30

Claims 3 and 30 serve to differentiate preceding claims (1-2 and 28-29, respectively) over Ontiveros, at least because Ontiveros only arguably mentions collection of packet counts which can be considered akin to statistical information on packets, as called for by claims 3 and 30, compelling the conclusion that Ontiveros does not the describe the connection features of claims 1-2 and 28-29, respectively.

Claims 8 and 9

Each of Claims 8 and 9 serve to further distinguish over Ontiveros.

Ontiveros does not describe the connection table and specifically the features of that the connection table includes a plurality of records that are indexed by source address. The memrefs described by Ontiveros are a single count of the number of packets with a particular source address.

Therefore, in addition to not possessing the claimed connection table structure, Ontiveros neither describes nor suggests the memrefs as a plurality of records or indexed by source address.

Similar arguments apply for claim 9 directed to indexing by destination address.

Claims 10-13, 31 and 32

Claim 10 requires that the connection table includes a plurality of records that are indexed by time. Similarly claim 11 includes time as an index on the connection table and claims 12 and 13 further have the connection table organized as a plurality of connection sub-tables to track data at different time scales (claim 12) and specific connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time (claim 13).

The examiner uses paragraphs [0040 to 0049] from Ontiveros.

> **[0040] With respect more specifically to the "hit-count" table, each time a data packet is received, a preferred algorithm as described herein creates a new reference index (if one does not already exist) or increments the existing reference (i.e., counting packets). For example, as shown at 100 in FIG. 2, the packet daemon identifies the packet source address qw1232ewr23 and at 102 creates a memory reference (memref) for that source address. At 104 the packet daemon identifies the source address of the next data packet traversing the port being monitored by the packet daemon, in FIG. 2, the source address being mg32ewr009. At 106 another memref is created for this source address. Therefore, at 104 each of the memrefs are equal to 1, representing that one data packet from each of the sources identified has traversed the data port of interest. At 108, another packet from source address gw123ewr23 is identified, and as shown at 110, the corresponding memref for that address is incremented. So, if for example the threshold data packet value is 1000 for the sample time (e.g., 10 milliseconds), and source address qw1232ewr23 exceeds the threshold in this period (e.g., memref qw1232wer23=1001), then access to the port being monitored will be denied to packets from that source. It should be noted that the source may be transmitting from either outside or inside the network.**

Ontiveros in [0040] discusses sampling time, as a threshold of access to a monitored port. However, Ontiveros does not describe any structure that stores records according to the sampling time. In contrast, claim 10 requires that the records are indexed by time. Thus, for an indexed time period records produced during that period can be accessed.

Claims 14 and 15

Claim 14 is directed to a method and includes the features of "sending connection information to an aggregator to identify host connection pairs collected from a plurality of collector devices; and producing in the aggregator a connection table that maps each node on the network to a record that stores information about traffic to the node and traffic from the node, with the connection table including a plurality of entries that are indexed by source address.

Claim 14 is not anticipated by Ontiveros at least because Ontiveros fails to describe the claimed connection table and those actions of sending connection information to an aggregator and producing a connection table that maps each node on the network to a record that stores information about traffic to the node and traffic from the node.

In addition, Ontiveros does not describe the connection table including a plurality of entries that are indexed by source address. The memrefs described by Ontiveros are a single count of the number of packets with a particular source address. Ontiveros therefore neither describes nor suggests the memrefs as a plurality of entries indexed by source address.

Claim 16

Claim 16 further limits claim 15 and includes determining from the connection information and the statistical information occurrences of network anomalies and aggregating anomalies into network events that indicate potential network intrusions and communicating occurrences of network events to an operator. Appellant also contends that Ontiveros fails to describe a process to detect anomalies in connection patterns and a process to aggregate detected anomalies into network events. (See discussion above).

Claims 18-22

Claims 18-22 include specific indexes to the feature of connection table (plurality of entries indexed by destination address (claim 18), ... indexed by time claim 19; ... indexed by source address, destination address and time claim 20, as well as ... a plurality of connection sub-tables to track data at different time scales (claim 21) and ... the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table

holding the sum of records received from all collectors during respective units of time (claim 22). These claims are allowable for reasons discussed in claim 14 and for analogous reasons discussed for claims 8-13, above.

Conclusion

Appellant submits that claims 1-25 are allowable over the art of record. Therefore, the examiner erred in rejecting Appellant's claims and should be reversed.

Respectfully submitted,

Date: January 22, 2008

/Denis G. Maloney/
Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

Appendix of Claims

1. A system, comprising:

a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network; and

an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node, with the aggregator device further comprising:

a process executed on the aggregator device to detect anomalies in connection patterns; and

a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

2. The system of claim 1 wherein the aggregator determines at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusions.

3. The system of claim 2 wherein the aggregator further comprises:

a process that collects statistical information on packets that are sent between nodes on a network and which sends the statistical information to the aggregator.

Claim 4 is canceled.

5. The system of claim 1 wherein the collector devices have a passive link to devices in the network.

Claim 6 is canceled.

7. The system of claim 1 wherein the anomalies include unauthorized access and worm propagation.

8. The system of claim 1 wherein the connection table includes a plurality of records that are indexed by source address.

9. The system of claim 1 wherein the connection table includes a plurality of records that are indexed by destination address.

10. The system of claim 1 wherein the connection table includes a plurality of records that are indexed by time.

11. The system of claim 1 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

12. The system of claim 1 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales.

13. The system of claim 12 wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time.

14. A method, comprises:

sending connection information to an aggregator to identify host connection pairs collected from a plurality of collector devices; and

producing in the aggregator a connection table that maps each node on the network to a record that stores information about traffic to the node and traffic from the node, with the connection table including a plurality of entries that are indexed by source address.

15. The method of claim 14 further comprising:

collecting statistical information in the collector devices to send to the aggregator device.

16. The method of claim 15 further comprises:

determining from the connection information and the statistical information occurrences of network anomalies; and

aggregating anomalies into network events that indicate potential network intrusions and communicating occurrences of network events to an operator.

Claim 17 is canceled.

18. The method of claim 14 wherein the connection table includes a plurality of entries that are indexed by destination address.

19. The method of claim 14 wherein the connection table includes a plurality of records that are indexed by time.

20. The method of claim 14 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

21. The method of claim 14 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales.

22. The method of claim 21 wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time.

Claims 23-27 are allowed.

28. A storage medium storing a computer program product, the computer program product comprising instructions for causing a computer to:

collect connection information to identify host connection pairs from packets that are sent between nodes on a network and produce a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node;

detect anomalies in connection patterns; and

aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

29. The storage medium of claim 28 further comprising instructions to determine at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusions.

30. The storage medium of claim 28 further comprising instructions to collect statistical information on packets that are sent between nodes on a network.

31. The storage medium of claim 28 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

32. The storage medium of claim 28 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales, the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time.

Claims 33-36 are allowed.

Evidence Appendix

None

Related Proceedings Appendix

None